FSA Security Incident Implementation Guide

October 2003

Table of Contents

FSA Security Incident Implementation Guide

1.0 INTRODUCTION

All Federal agencies are required by law to have within their information technology (IT) security programs an incident handling and reporting capability. FSA and its contracted partners operate a large number of systems at numerous locations using many different software platforms. While these systems are constructed securely, security incidents will inevitably occur.

1.1 Purpose

This document directly addresses FSA's roles, responsibilities, and expectations for responding to security incidents, and provides specific instructions on how to meet the requirements of the Incident Handling Guide from the Department of Education's Education Computer Incident Response Center (EDCIRC). FSA maintains a unique dependence on variety of contractors to operate its systems that is not found elsewhere in the Department of Education, hence the need for more specific, FSA-level guidance.

FSA's primary responsibility is to report incidents and suspicious activities to EDCIRC according to the reporting guidelines contained in Appendixes B and C of the Incident Handling Guide. After receiving such a report, EDCIRC then provides investigative, forensics, and analysis capabilities for most, if not all systems. FSA is also responsible for responding to additional EDCIRC requests that result from these investigations.

1.2 Scope

This Implementation Guide is designed to help FSA personnel understand their roles and responsibilities in the incident response process. It includes plans for notifying affected parties, escalating responses through the chain-of-command, and coordinating with the Departmental incident response team (if necessary). It is important that security personnel (eg, system security officers) and those who work directly with computer systems understand and follow this document.

Note: The EDCIRC documents on incident response are the primary sources that must be consulted and followed; this document is a supplement to EDCIRC incident response guidelines, providing FSA-level detail where necessary to meet the sometimes more general EDCIRC requirements.

1.3 Document Structure

The document is divided into four sections and an appendix. Section 1.0 is an introduction and provides important definitions. Section 2.0 discusses incident prevention. Section 3.0 deals with the monitoring and review of system and network logs. Section 4.0 describes the specifics for FSA on security incident reporting, including a discussion on communicating security incidents, the detailed responsibilities of each of the affected parties, and how they interact with each other. Section 5.0 focuses on the

reporting of suspicious activity, including the necessary steps and reports and the required timeframes.

1.4 Definitions

An effective Incident Response Program requires that certain terms be defined in a precise way to avoid confusion. FSA utilizes the Department's definitions as the baseline and also provides clarification by providing industry-recognized definitions; these are predominately based on the National Security Agency (NSA) National Security Telecommunications and Information Systems Security Committee (NSTISSI) 4009 document.

These definitions give basic qualifying information for identifying security incidents and suspicious activities. This information must be combined with common sense, discretion, and diligent professional interpretation of any activity in order to adequately identify incidents or suspicious activity.

Computer Security Incident and Suspicious Activity Definitions

Computer Security Incident (EDCIRC)	*Any event that has resulted in: unauthorized access to, or disclosure of, sensitive information; unauthorized modification or destruction of system data; reduced, interrupted, or terminated data processing capability; introduction of malicious program or virus activity; or the degradation or loss of the system's Confidentiality, Integrity or Availability; or the loss, theft, damage, or destruction of an IT resource.* Examples of computer security incidents include: unauthorized network scans or probes; successful and unsuccessful system intrusions; unauthorized use of system privileges; and, execution of malicious code on an IT resource. (See Schedule A -- Incident Reporting & Response Guidance: Types of Incidents Matrix for more examples.)
Suspicious Activity (EDCIRC)	*Any activity that is considered: an abnormal system event occurrence for a given system that cannot be immediately explained, but does not pose an immediate threat; observed recurring activity that possibly indicates attempts are being made to exploit a vulnerability but is countered by security controls in place; sporadic repeated activity that cannot be readily explained by system operations and security staff; activity that, when combined with other factors or anomalous events,* ***indicates a possible cause for concern****.* Examples of suspicious activity include: unusual usage patterns, misuse of computer system resources, or multiple attempts to log into a user account that have proven unsuccessful. (See Schedule B -- Incident Reporting & Response Guidance: Types of Incidents Matrix for more examples.)

The above definitions should be sufficient to identify security incidents and suspicious activities. However, for more precise definitions of security incidents and to see how such incidents fit into FSA's overall information assurance program, see the table below.

NSTISSI 4009 Computer Security Incident Definitions

Term		Definition
Information Assurance (NSTISSI 4009)		Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.
IA INCIDENT TYPES	**Attack**	Involving the intentional act of attempting to bypass one or more information assurance (IA) security controls of an information system (IS).
	Compromise	Where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized internal or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
	Contamination	Involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.
	Denial of Service (NSTISSI 4009)	Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.
Compromised System (Based on NSTISSI 4009)		A system for which security measures fail to provide IA.
Security Incident (Based on NSTISSI 4009)		An assessed occurrence resulting in a compromised system. This means that at least one the IA incident types was not stopped by currently implemented security measures.
A security incident occurs *only* when security policies and implementations fail to protect a system from one of these industry-recognized standards.		

One of FSA's primary information assurance goals is maintaining information system integrity, availability, authentication, confidentiality, and non-repudiation. Incident response is an important part of information assurance because it addresses the actions that need to occur when information is compromised.

2.0 INCIDENT PREVENTION

"An ounce of prevention is worth a pound of cure" is an old saying, but one that is particularly true for IT infrastructure. Practical experience has proven that the large majority of computer incidents can be avoided by taking small, appropriate, and timely measures. All FSA systems are required to prevent incidents by deploying proven software and devices, including anti-virus products, intrusion detection systems and devices, firewalls, IT security awareness training, and patch management tools and techniques. Section 3.8 of FSA's Information Technology Security and Privacy Policy (FSA Security Policy), Incident Response, also underlines the need for preventative security. However, all preventative measures and devices will be effective *only* if 1) the system uses appropriate security measures – devices or software - according to its use and needs and 2) the software and devices are properly updated, patched, and configured.

Patch management techniques and tools are therefore essential to incident prevention. On the one hand, properly deployed and patched/updated software or hardware is difficult to compromise. On the other hand, improperly or unpatched/nonupdated items are the primary reasons for a security incident. The following section discusses the patch and update management considerations at FSA

2.1 Patch and Update Management

Patch management is only one component of security management in general, as the confidentiality, integrity, and availability of FSA systems depends in large part on the preventative security measures taken to deter or inhibit attacks. More specifically, patch management is a subset of configuration and change management processes. As mentioned above, patch management is also closely linked to incident response.

Section 3.7 of the (FSA Security Policy) specifically addresses configuration/change management. Further, all FSA systems have configuration management plans that adhere to the Departmentwide configuration management guide.

In addition to rapidly report on system coverage, FSA is increasingly being required to also report on the level of each system's specific patch and update coverage. This suggests the need for automated patch management tools, which can easily and quickly supply such information for large networks.

To help meet current Federal requirements, FSA has established an email alert process that informs system personnel of new security fixes, patches, and problems. It has also established a process for tracking and reporting implementation compliance for patches and fixes.

2.2 Procedures for IT Security Alerts

The FSA Security and Privacy Team (S&P Team) issues two categories of IT security alerts -- low-to-medium-level threats and high-level threats (these are also identified as critical alerts). Each category requires action by an FSA contractor and/or the system's

System Security Officer (SSO). Although the low-to-medium alerts are of interest and require appropriate action, these actions can usually be scheduled so they do not interfere with normal business operations. On the other hand, high-level, or critical alerts need immediate action to prevent an imminent security incident that could deny access, release private citizens' data, damage the Department's reputation, or incur major expenses for reconstitution of the system.

2.2.1 Low-to-Medium Alerts

The FSA S&P Team regularly forwards IT security alerts to the SSOs for all FSA systems. These alerts are routinely disseminated on Tuesdays and Fridays, and normally contain a mixture of low- and medium-level vulnerabilities. When the routine Tuesday and Friday alerts are issued, SSOs are expected to pass the information on to the technical support staff for the system, be it a government employee or contractor employee. Together with such staff, the SSO will determine which of the alerts indicates a risk to their system, and take appropriate action to prevent the threat or attack from affecting the system. There is no requirement to report on the status of any given threat/vulnerability/remediation effort, though the SSO should be ready to respond to inquiries concerning an alert.

2.2.2 Critical Alerts

When a high-level, or critical alert is issued by FedCIRC, OMB, a manufacturer, or another source, the FSA S&P Team will *immediately* issue the alert to both the appropriate SSOs and contractor contacts. For systems residing at the Virtual Data Center (VDC), CSC staff (the contractors who run the VDC) will be notified, along with the VDC SSO. The SSO and contractor contacts for systems with components external to the VDC will also be notified. A list of contacts for the alerts is maintained by the FSA CSO. SSOs should check with the CSO to update the contact information for their systems. Periodically, the list will be disseminated for updating, but changes to the contact list should be forwarded to the S&P Team as soon as they are applicable.

- High-level or critical alerts will be issued by email (first line of alert) and by telephone (second line for follow up, and when an email acknowledgement has not been provided). When an alert requires immediate action , the email message will bear a specific title, such as that shown below:

    - **Special Threat Alert & Response (STAR) – Immediate Action Required**

    - The opening paragraph of the alert will provide a description of the special action needed as well as a reminder of the contact information for people in the S&P Team. Technical details of the alert will be included in the email message, either as text or as a file attachment.

- When a **"STAR"** alert is issued, the "owners" of the IT systems to which the alert is directed are responsible for reporting the status of remediation efforts. This reporting can be done by either the SSO or the contractor contact. In either case, the other party must be included as a cc: for the message.

- An FSA reporting form identifying the number of affected components, the number of fixes, and dates, along with other pertinent information, will be included with each new STAR alert. If there are special reporting formats required by OMB, ED CIO, or other government agency with oversight responsibility, they also will be provided with the alert.

- A report must be filed within 2 hours of receipt of the alert. The report should be sent to the S&P Team member who sent the alert. The initial report can be a simple acknowledgement that the alert was received. Remediation decisions, installation of system patches or work-arounds, and other pertinent status information will be conveyed in timely followup reports. Upon occasion, government agencies or offices with oversight responsibility may request reports within a shorter time period.

- In any case, reporting and remediation of critical vulnerabilities will be given high priority by the system owner and system manager, and any decision to delay actual remediation (by using work-arounds) must be agreed to by the system manager. If sound business reasons exist to delay applying a patch or installing an upgrade that could/would remediate the threat/vulnerability, the system manager must state in writing the reason for the delay and must obtain concurrence of the FSA CIO.

- When a work-around is used in place of full remediation, the status for that system will be kept "open" until remediation is accomplished. Both ongoing remediations as well as a final report should be filed once full remediation is accomplished.

2.3 Tracking

The FSA S&P Team will maintain a data system that allows the status of each critical vulnerability to be tracked for each system.

3.0 MONITORING SYSTEMS, KEEPING AND REVIEWING LOGS

Audit logs are critical to incident response activities. Periodic review of audit logs helps technical personnel establish a baseline of system activity. Once the personnel have an idea of the baseline, it makes it easier to recognize anomalies in subsequent log reviews. Early identification of anomalies consequently makes it easier to proactively defend the system from attackers.

The following items are the minimum requirements for all systems in regards to monitoring, logging, log review, and log retention:

- Maintain sufficient monitoring/logging capability (see Department guidelines)
- Establish typical activity levels or thresholds for system events on each system.
- Monitor and log all systems and system activities (see Department guidelines).
- Someone familiar with the system must review all systems logs and audits at least once a day for any events or series of events that could indicate a breach in security.
- Document the review.
- Each system must retain a copy of all audit logs. Section 4.3 of the FSA Security Policy states that such logs will be kept for a minimum of 1 year.
- Remain alert for behavior that is obviously out of place or wrong (eg, web defacements and denial of service attacks).

To avoid confusion, FSA refers to the routine inspection of logs and audits for suspicious activities or security incidents as a "log review." Log reviews can be accomplished through automated and/or manual methods and tools. The terms "analysis" and "log analysis" refer to a scrutinized inspection of data, logs, and audits after a suspicious activity or incident has been identified.

3.1 Security Incident versus Suspicious Activity

"What are we looking for?" is the first question that is commonly asked when thinking about incident response. Typically, one looks for activity on the logs that does not follow the general rules of the system—however, such activity does not necessarily constitute "suspicious activity" or a "security incident". Therefore, only a general description and some possible examples of what to look for can be given here.

The reality is that each FSA system has different "normal" activity levels and different "normal" toleration levels for certain types of activities that only those familiar with the system will know. That is why it is important to establish a baseline activity log. If the noted activity is different or crosses specified thresholds, or is of a distinctly different nature, then there is probably good cause for concern and gives reason to call the event "suspicious activity."

Actually identifying an issue of concern as a "security incident" entails being able to positively know and/or show that a compromise has occurred. Moving an issue previously considered a "suspicious activity" into the category of a "security incident" requires research and analysis.

4.0 REPORTING SECURITY INCIDENTS

The following table provides a concise view of what actions *all* stakeholders should take in response to security incidents (These steps are described in greater detail in section 4.1 below). The activities are presented chronologically starting with row one (1). Note that in rows 8 and 11, actions start in the EDCIRC column.

4.0 Table – Security Incident Handling Process

Contractors	FSA	Ed or EDCIRC	
1) Monitor and review systems and logs			
2) Identify security incident			
3) Immediately notify FSA for authority to take system off-line	**3a)** Approve system to go off-line and notify EDCIRC of decision		
4) If instructed, take system off-line, isolate, and freeze			
5) Complete incident form and follow reporting chain. (See Diagram 3.2)	**5a)** SSO reviews report, relays it to CSO; CSO relays it to EDCIRC	**5b)** Reviews report – provide feedback and "next-step" information; notify FEDCIRC and others as necessary	
6) Follow instructions from EDCIRC	**6a)** Follow instructions from EDCIRC		
7) Provide status on actions taken	**7a)** Receive contractor status	**7b)** Receive contractor status	
		STATUS REPORTS	**8)** Analyze incident data and system, conduct forensics/ investigate
9) Propose alternate/backup system; wait for approval	**9a)** Receive and approve alternate request		
10) Implement alternate System			
11b) Receive Findings Report; consult on course of action	**11a)** Receive Findings Report; consult on course of action		**11) Complete a**nalysis and submit findings; propose course of action
12) Follow and complete course of action			
13) Resolve security incident, request system reestablishment, wait for approval.	**13a) Approve s**ystem reestablishment		
14) Document lessons learned			

Section 4.1 below, provides a detailed description outlined in the table above. (Refer to the FSA Incident Response Contact List for contact information. See also Figure 4.3, FSA Security Incident Reporting Chain, and Table 4.2, Security Incident Reporting Chain, Timeline Summary). Please note that while contractors, FSA, and the Department must all work together for resolution, each group has specific responsibilities.

4.1 FSA Security Incident Reporting: Process Details

(For summary information refer to: Table 4.0, Table 4.2, and Figure 4.3)

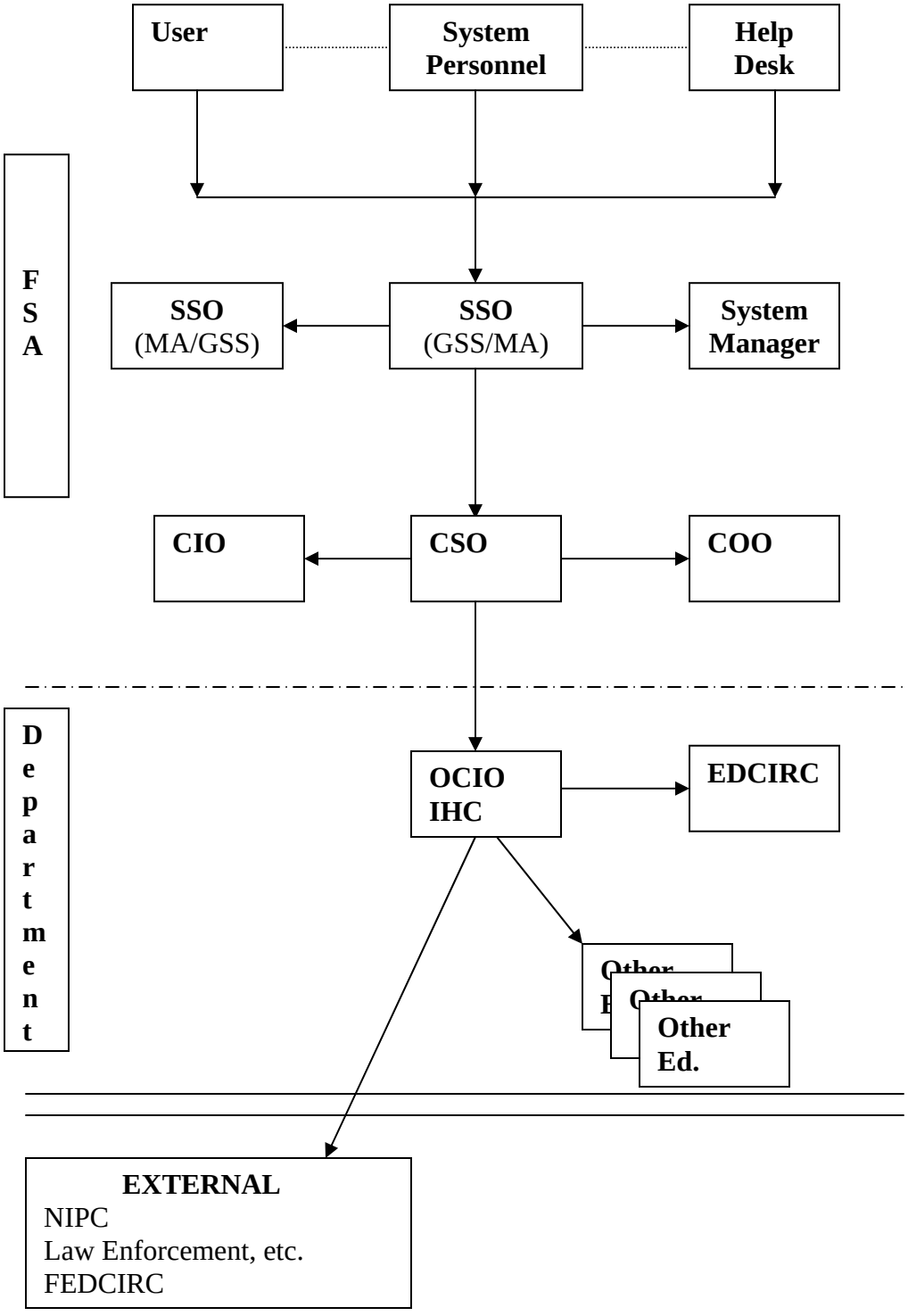
- Any observed activity that may indicate a computer security incident has occurred must be reported immediately to the relevant SSO or security administrator by telephone, email, or fax. The reporting party must receive "confirmation of receipt" from the relevant SSO or security administrator; it is the responsibility of the reporting party to note the time receipt was confirmed. *If the relevant SSO or Security Administrator is not available by telephone, email, or fax, the reporting party must notify FSA's CSO using the same process and receipt confirmation. Likewise, if the CSO or his alternate is not available then the reporting party must notify the Department's Incident Handling Coordinator directly*. (See Appendix A for contact information. Also, see the attached Suspicious Event Report (SER) form for the information that should be reported.) SSOs, Computer Security Officers (CSOs), and other FSA staff will be trained concerning observable indicators that suggest an incident may have occurred.
- The SSO will ensure that all information on the SER form has been filled out. The SSO must then notify FSA's CSO or Deputy CSO by telephone, email, or fax within **1 hour** of receiving the initial SER form. *If the CSO has not confirmed receipt within 1 hour of notification, the reporting party must notify the Deputy CIO using the same process and receipt confirmation.*
- If it is a General Support System (GSS) that reports the security incident, then the SSO for that GSS will notify the SSO(s) of any and all major applications (MAs) directly affected by that particular GSS, and will keep those SSOs informed for the duration of the incident. If it is an MA that reports the security incident, then the SSO for that MA will notify the SSO(s) of the GSS that supports the MA, and will keep that SSO informed for the duration of the incident.
- The reporting SSO will also notify the appropriate System Manager
- The CSO reviews the initial SER form and related information to determine whether a potential incident has occurred. The CSO then reports the potential incident and all related information to the Office of the Chief Information Officer (OCIO) Incident Handling Coordinator within **3 hours** of receiving the initial report. All information will be included in a report to the OCIO Incident Handling Coordinator.

- The CSO will at the same time notify and send a report to both the CIO and COO.
- The OCIO Incident Handling Coordinator will make a determination for next steps using the Department's incident handling program procedures **within 1 hour of receiving a SER**. If warranted, the Incident Handling Coordinator may escalate the details of the report to the Deputy CIO. If the security event or suspicious activity is deemed a serious threat to any Department's IT resources or data, the OCIO Incident Handling Coordinator will activate the Education Computer Incident Response Capability (EDCIRC) procedures and escalate the information to the Deputy CIO.
- The Deputy CIO will review the SER **within 1 hour** of receipt and determine whether escalation to the CIO is warranted.
- The CIO or the CIO's designee will review the SER within **1 hour** of receipt and determine whether escalation to the Deputy Secretary, the Office of the Inspector General, and appropriate external officials is warranted.

4.2 Security Incident Reporting Chain: Timeline Summary

Position	**Reports To**	**Required Response Time**
System Administrator	SSO	Immediately
SSO	FSA Incident Coordinator or CSO	1 hour
CSO	Dept. OCIO Incident Handling Coordinator and PO Senior Officers	3 hours
Dept. OCIO Incident Handling Coordinator	Deputy Chief Information Officer	1 hour
Deputy Chief Information Officer	Chief Information Officer	1 hour
Chief Information Officer or Designee	Deputy Secretary, Inspector General, and others as appropriate	1 hour

4.3 FSA Security Incident Reporting Chain



4.4 Post reporting Actions and Expectations

Once an actual incident is recognized and reported, all affected parties must continue to support, cooperate, and communicate with each other. EDCIRC (or whoever is providing analysis services) will collect data and research the extent of the problem to determine if there are additional suspicious activities or security incidents. This is accomplished primarily through in-depth log and audit analysis. The Contractor must assist and support EDCIRC in this process by immediately providing all details and information as needed or requested.

4.5 Preservation of Evidence

Proper handling of a computer after an incident has been identified is critical. Once a system has been taken off-line with the concurrence of a government authority and the coordination of the Incident Handling Coordinator, that system will not be tampered with in any way or brought back on line without authorization from both FSA's and the Department's Incident Handling Coordinators. This is necessary to preserve potential criminal evidence and the system condition at the time an incident was discovered.

4.6 Alternate Connectivity

FSA expects contractors to provide an alternate, secure system that clients may continue to access during extended investigations.. Such an alternate system will be activated only upon agreement between FSA Incident Handling Coordinators, consistent with FSA's Continuity of Support Plan (COS) and the Disaster Recovery Plan (DR). Some systems with low availability ratings may not have a COS or DR that calls for alternate system processing. In such cases the contractor should make that information known and consult with FSA on how to proceed. The alternate processing proposal should be submitted as soon as possible. FSA and the Departmental authority must approve the proposal for the alternate system before it is placed on-line.

4.7 Three-Way Consulting

After receiving the findings information from a completed investigation/analysis, the Contractor must consult with FSA and the Department and propose a course of action to remedy the problem and prevent its reoccurrence. FSA, Department, and Contractor parties must agree on the course of action before implementation.

4.8 Final Status

Once the security incident is resolved, and the agreed-on course of action is completed, the Contractor will request approval to reestablish the system (or approval to show final disposition if the system is not reestablished). The Contractor must wait until consent is given by Incident Response Coordinators before reestablishing or otherwise disposing of any system involved in a security incident.

5.0 REPORTING SUSPICIOUS ACTIVITY

The following table shows, in chronological order (starting with "1"), the steps stakeholders must take when reporting suspicious activity (these steps are described in greater detail in section 5.1 below). Please note that the actions in rows 5 and 6 start in the EDCIRC column.

5.0 Suspicious Activity Handling Process

Contractors	FSA	Ed or EDCIRC
1) Monitor and review systems and logs		
2) Identify suspicious activity		
3) Leave system on-line		
4) -Prepare In Month Report - Category A activities -Prepare In Week Report - Category B activities	**4a)** SSO reviews report and relays it to CSO; CSO relays report to EDCIRC	**4b)** EDCIRC reviews report
		5) Analyze activity 1) Allowed activity 2) Inconclusive – mark and monitor 3) Security incident (see s section 4.3)
6b) Take action as advised by EDCIRC.	**6a)** Receive action and feedback report from EDCIRC	**6)** Provides analysis feedback and required action to FSA and Contractor

Section 5.1 below, provides a detailed description outlined in the table above. It should be noted that reporting suspicious activity is quite different from reporting security incidents. Suspicious activity requires that a report be filed within 1 week or 1 month depending on the category of suspicious activity (Category B within 1 week and Category A within 1 month). (See also the Department's Incident Handling Guide, Appendixes, Reporting Guidance, Schedule A and B).

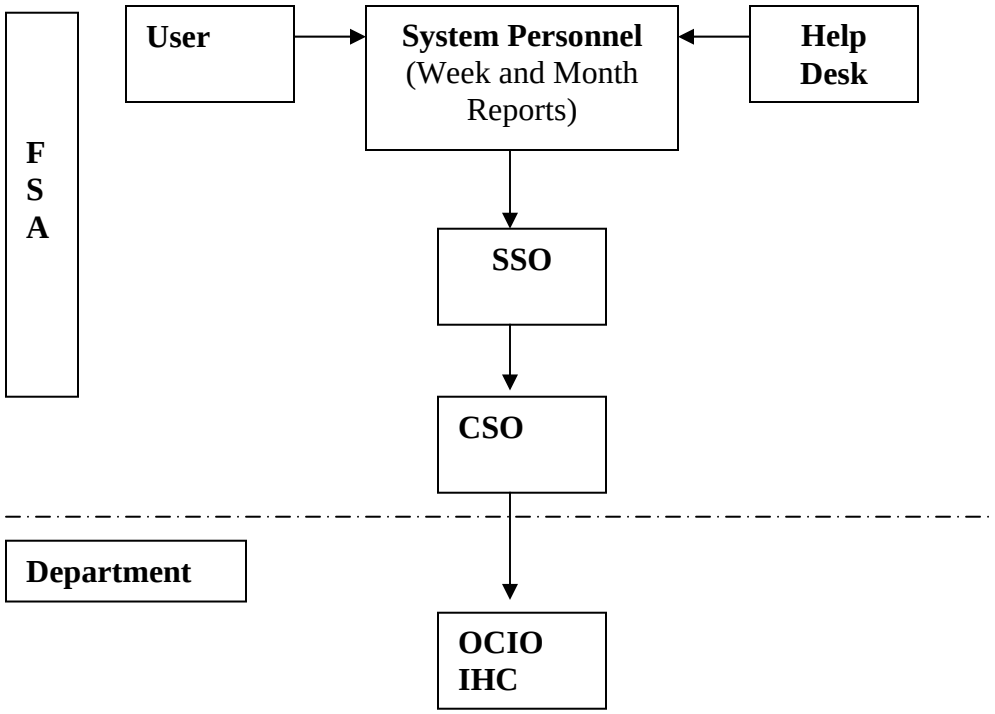
5.1 'Suspicious or Anomalous Activity' Reporting: Process Details

(For summary information refer to Table 5.0, Figure 5.2, and Table 5.3)

Follow the Suspicious Activity Reporting Chain in section 5.2 when using the Incident Response capabilities provided by EDCIRC. (Note: Even if an FSA Contractor is *not* using EDCIRC services, the reporting requirements remain the same. This also means that Contractors will report their analysis, findings, and recommendations to the SSO (who will forward the information to the CSO) within the specified timeframe to show that items are being resolved.)

- If a system log review indicates suspicious activity, the reviewer will report it to the Security Engineer through the internal contractor channels, and also to the SSO, who will categorize the activity according to Schedule B --Incident Reporting & Response Guidance: Suspicious Activity.
- Category "A" type suspicious activity (activity that is effectively countered by security controls in place) will be logged and tracked by the system SSO. The SSO will provide a report on Category A activity to the CSO within 1 month. Please note that a report can be submitted at any time if there is special concern over a given activity.
- Category "B" type suspicious activity (activity that is effectively countered by security controls in place, but its continued repetition causes additional concern) will be reported by the SSO to the CSO within 1 week. Please note that a report can be submitted at any time if there is special concern over a given activity.
- The CSO will review and then forward all suspicious activity reports to the Department's Incident Handling Coordinator, who will review the reports and relay any findings and recommended action to the submitting office within **24-48 hours** of receipt.

5.2 FSA Suspicious Activity Reporting Chain



5.3 Suspicious Activity Reporting Chain, Timeline Summary

Position	Reports To	Category A Response Time	Category B Response Time
System Administrator	System Security Officer (SSO)	Within 1 month	Within 1 week
System Security Officer (SSO)	Computer Security Officer (CSO)	Within 1 month	Within 1 week
Computer Security Officer (CSO)	OCIO Incident Handling Coordinator	Within 1 month	Within 1 week
OCIO Incident Handling Coordinator	Back to originating office	24 to 48 hours	24 to 48 hours

5.4 Post reporting Actions and Expectations

Once suspicious activity is recognized and reported, all affected parties must continue to support, cooperate, and communicate with each other. The contractor may be asked to compile more data to help researchers determine the extent of the problem and identify any additional suspicious activities or security incidents. The Contractor must be ready to cooperate with EDCIRC in this process and immediately provide all details and information as needed or requested.

In the case of suspicious activity, further analysis will show one of three conclusions: a security incident, no cause for concern, or unknown and/or inconclusive requiring monitoring. If the suspicious activity is concluded to be a security incident, then the process and procedures for a security incident found in this document shall be followed. The actions to take for the two remaining conclusions are self-defining **[NEED TO BE MORE SPECIFIC THAN THIS—EG, "NO FURTHER ACTION IS REQUIRED"; "MONITOR THE SITUATION BY DOING X, Y, AND Z, ACCORDING TO THE POLICIES IN XX]**.

6.0 Providing All Incident Response Services

Providing all incident response services means incorporating into one program the analysis, forensics, and remediation of any security incident or suspicious activity, in addition to the monitoring, reviewing, identifying, and reporting tasks. Such a program must follow the same process in the Department's Incident Handling guide. Anything more or less must be approved in advance by EDCIRC.

FSA currently provides only a basic portion of the incident response services and relies on the Department's program for analysis, forensics, and remediation support.

For informational purposes, the following list shows a high-level outline of tasks that are necessary in providing total "in-house" incident response capabilities:

- Monitoring
- Incident prevention
- Review of logs and audits
- Identification
- Reporting
    - Security Incidents
    - Suspicious Activity
        - Weekly Report
        - Monthly Report
- Analysis of reports, logs, audits, and data
- Forensics (including legal evidence-handling procedures)
- Remediation plan

APPENDIX A - FSA SECURITY INCIDENT CONTACT LIST

Important Notice:

The following FSA Security Incident Contact List is to be used only for FSA Security Incident Response purposes. It is not to be made public or shared with those outside of the Incident Response program.